ASUS RT-G32 rev. C1 and RT-N10 rev. B1

By Maxim Klimanov and MIPT DREC students

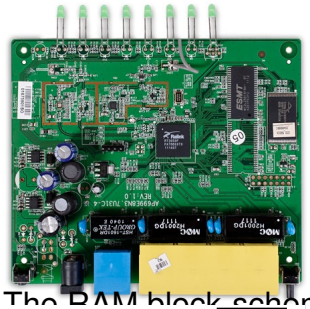
Introduction

Today we're presenting to you a review of two wireless routers ASUS RT-N10 rev.B1 and ASUS RT-G32 C1 which are in many ways similar to RT-N10U but are still different from it. ASUS RT-N10 B1 and ASUS RT-G32 C1 are low-cost devices supporting several wireless networks simultaneously with similar technical parameters; thus we decided to review them together.

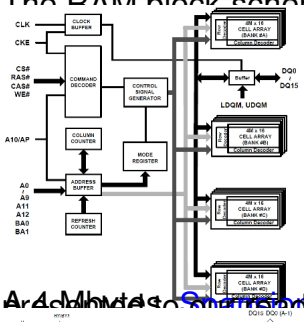
External design and hardware

The RT-N10 rev.B1 wireless router is performed in a black plastic case whereas RT-G32 rev.C1 is in a white one; other design features are the same.

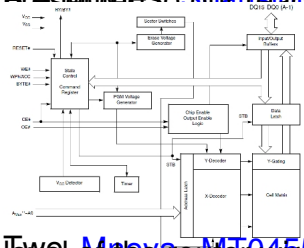
MSoC chip Ralink RT3050F performs the functions of CPU. RAM is represented by a 32 Mbyte Etron EM63A165TS-6G module working at 166 MHz frequency.



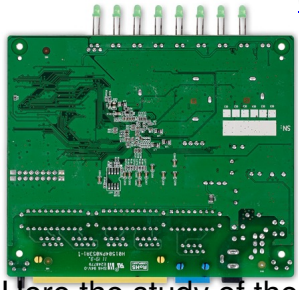
The RAM block-scheme is presented below.



A 4 Mbyte Spansion S29GL032N chip was used as flash-memory; its block-scheme is also standard.



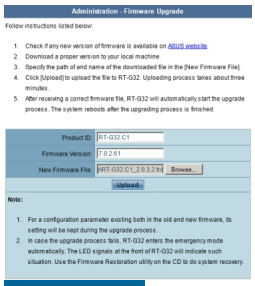
Two Mnova MT0455 and one Mnova MT0454 transformers are responsible for the physical part.

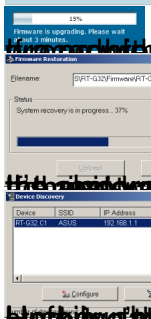


Here the study of the hardware part is over and now let's look at the routers' software features.

Firmware upgrade and restoration

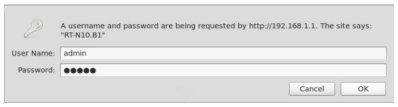
One can change a firmware version with the help of the "Firmware Upgrade" tab of the "Administration" menu in the device web-interface. The whole upgrade process takes about three minutes.


Administration - Firmware Upgrade
Follow instructions listed below:
1. Check if any new version of firmware is available on ASUS website.
2. Download a proper version to your local machine.
3. Specify the path of and name of the downloaded file in the [New Firmware File].
4. Click [Upload] to upload the file to RT-G32. Uploading process takes about three minutes.
5. After receiving a correct firmware file, RT-G32 will automatically start the upgrade process. The system reboots after the upgrading process is finished.
Product ID: RT-G32.C1
Firmware Version: 7.0.2.61
New Firmware File: RT-G32.C1_2.0.3.2.trx
Browse...
Upload
Note:
1. For a configuration parameter existing both in the old and new firmware, its setting will be kept during the upgrade process.
2. In case the upgrade process fails, RT-G32 enters the emergency mode automatically. The LED signals at the front of RT-G32 will indicate such situation. Use the Firmware Restoration utility on the CD to do system recovery.

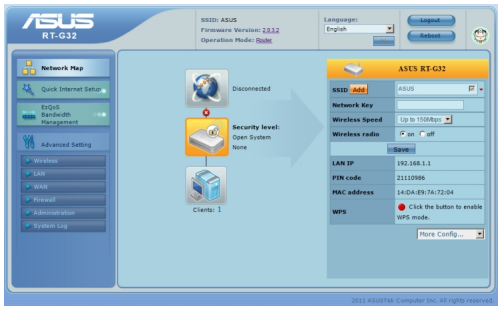


Web-interface review

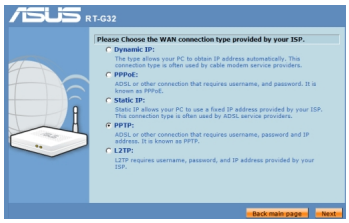
To access the router homepage, the user has to get to 192.168.1.1. Then account data is required – login and password (admin/admin). The device web-interface is available in twelve languages among which are Malaysian, Tai, and Turkish.



In the Network Map menu there're three sections: Internet connection status, security and the list of clients.

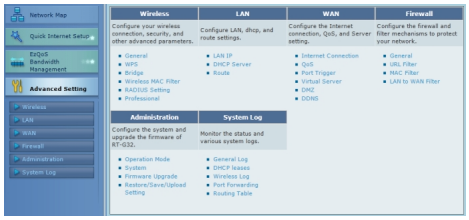


Let’s turn to the Quick Internet Setup tab that allows the user to easily configure the router main parameters for accessing the Global net.



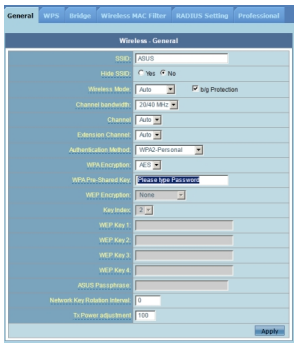
Also on the router homepage there’s an item EzQoS. The EzQoS program provides four types of popular internet-applications and makes quality of service (QoS) configuration quite simple.

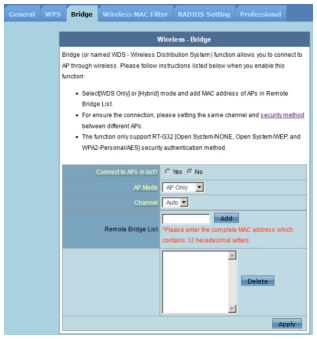
Now let’s study the Advanced Setting group of the main menu.

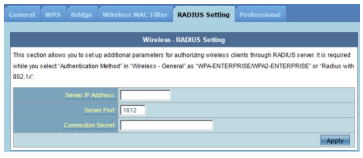


The Wireless group allows specifying the Wi-Fi module operation parameters. The General tab

of this group contains the settings for the main network. The Bridge tab allows one to activate the bridge function which lets you connect to other access points via a wireless net.




General
WPS
Bridge
Wireless MAC Filter
RADIUS Setting
Professional
Wireless - Bridge
Bridge (or named WDS - Wireless Distribution System) function allows you to connect to AP through wireless. Please follow instructions listed below when you enable this function:
Select[WDS Only] or [Hybrid] mode and add MAC address of APs in Remote Bridge List.
For ensure the connection, please setting the same channel and security method between different APs.
The function only support RT-G32 [Open System/NONE, Open System/WEP, and WPA2-Personal/AES] security authentication method.
Connect to APs in list
Yes
No
AP Mode
AP Only
Channel
Auto
Add
Remote Bridge List
*Please enter the complete MAC address which contains 12 hexadecimal letters.
Delete
Apply

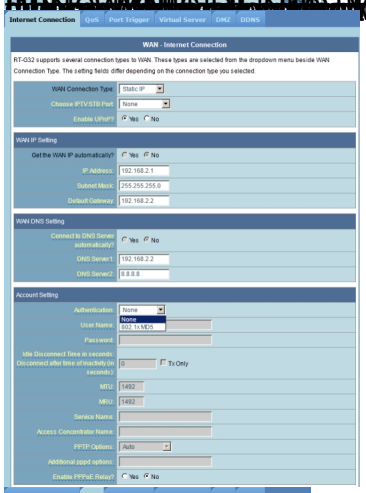

General
WPS
Bridge
Wireless MAC Filter
RADIUS Setting
Professional
Wireless - RADIUS Setting
This section allows you to set up additional parameters for authorizing wireless clients through RADIUS server. It is required while you select "Authentication Method" in "Wireless - General" as "WPA-ENTERPRISE/WPA2-ENTERPRISE" or "Radius with 802.1x".
Server IP Address
Server Port
1812
Connection Secret
Apply

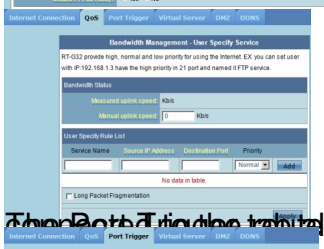
The Professional tab allows the user to configure advanced parameters of the wireless net.

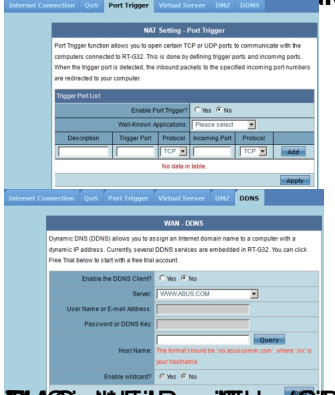
General
WPS
Bridge
Wireless MAC Filter
RADIUS Setting
Professional
Wireless - Professional
Wireless Professional Setting allows you to set up additional parameters for wireless. But default values are recommended.
Enable Radio?
Date to Enable Radio
Time of Day to Enable Radio
Set AP Isolated?
Multicast Rate(Mbps)
Basic Rate Set
Fragmentation Threshold
RTS Threshold
DTIM Interval
Beacon Interval
Enable TX Bursting?
Enable Packet Aggregation?
Enable Greenfield?
Enable WMM?
Enable WMM No-Acknowledgement?
Enable WMM APSD?
Enable WMM DLS?
Apply

LAN IP
DHCP Server
Route
LAN - LAN IP
Configure the LAN IP of RT-G32. The DHCP Server dynamically changes the IP pool when you change the LAN IP.
IP Address
Subnet Mask
Apply

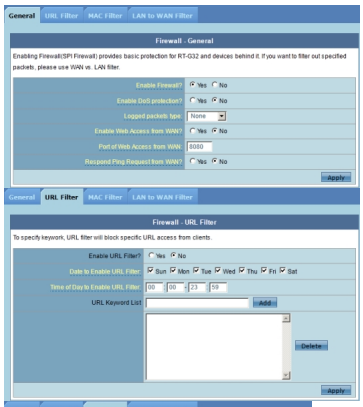
LAN IP
DHCP Server
Route
LAN - Route
This function allows you to add routing rules into RT-G32. It is useful if you connect several routers behind RT-G32 to share the same connection to the Internet.
Static Route List
Use DHCP routes?
Enable multicast routing?
IPTV/UDP Multicast to HTTP Proxy Port
Enable static routes?
Network/Host IP
Netmask
Gateway
Metric
Interface
Add
No data in table.


Internet Connection
QoS
Port Trigger
Virtual Server
DMZ
DDNS
WAN - Internet Connection
RT-G32 supports several connection types to WAN. These types are selected from the dropdown menu beside WAN Connection Type. The setting fields differ depending on the connection type you selected.
WAN Connection Type
Choose IPTV STB Port
Enable UPnP?
WAN IP Setting
Get the WAN IP automatically?
IP Address
Subnet Mask
Default Gateway
WAN DNS Setting
Connect to DNS Server automatically?
DNS Server1
DNS Server2
Account Setting
Authentication
User Name
Password
Idle Disconnect time in seconds
Tx Only
MTU
MRU
Service Name
Access Concentrator Name
PPTP Options
Additional pppd options
Enable PPPoE Relay?

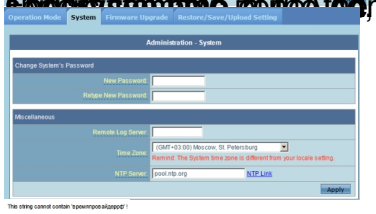

Internet Connection
QoS
Port Trigger
Virtual Server
DMZ
DDNS
Bandwidth Management - User Specify Service
RT-G32 provide high, normal and low priority for using the Internet. EX. you can set user with IP 192.168.1.3 have the high priority in 21 port and named it FTP service.
Bandwidth Status
Measured uplink speed
Manual uplink speed
Kb/s
User Specify Rule List
Service Name
Source IP Address
Destination Port
Priority
Normal
Add
No data in table.
Long Packet Fragmentation

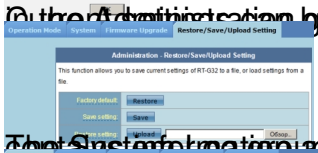

Internet Connection
QoS
Port Trigger
Virtual Server
DMZ
DDNS
NAT Setting - Port Trigger
Port Trigger function allows you to open certain TCP or UDP ports to communicate with the computers connected to RT-G32. This is done by defining trigger ports and incoming ports. When the trigger port is detected, the inbound packets to the specified incoming port numbers are redirected to your computer.
Trigger Port List
Enable Port Trigger
Well-Known Applications
Please select
Description
Trigger Port
Protocol
Incoming Port
Add
No data in table.
Apply

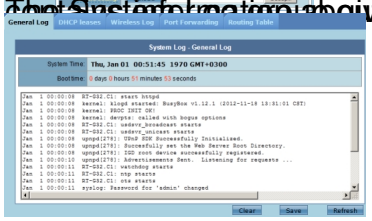
Internet Connection
QoS
Port Trigger
Virtual Server
DMZ
DDNS
WAN - DDNS
Dynamic DNS (DDNS) allows you to assign an Internet domain name to a computer with a dynamic IP address. Currently, several DDNS services are embedded in RT-G32. You can click Free Trial below to start with a free trial account.
Enable the DDNS Client?
Server
WWW.ASUS.COM
User Name or E-mail Address
Password or DDNS Key
Host Name
Query
Enable wildcard?


General
URL Filter
MAC Filter
LAN to WAN Filter
Firewall - General
Enable Firewall?
Enable DoS protection?
Logged packets type:
Enable Web Access from WAN?
Port of Web Access from WAN:
Respond Ping Request from WAN?
Apply
Firewall - URL Filter
Enable URL Filter?
Date to Enable URL Filter:
Time of Day to Enable URL Filter:
URL Keyword List:
Add
Delete
Firewall - MAC Filter
MAC Filter Mode:
MAC address:
MAC filter list:
Firewall - LAN to WAN Filter
Enable LAN to WAN Filter?
Filter table type:
LAN to WAN Filter Table
Source IP
Port Range
Destination IP
Protocol
TCP

Operation Mode
System
Firmware Upgrade
Restore/Save/Upload Setting
System Setup - Operation Mode
Wireless Router / IP sharing mode
Repeater mode
Access Point(AP) mode
Wireless Client
RT-G32
Modem


Operation Mode
System
Firmware Upgrade
Restore/Save/Upload Setting
Administration - System
Change System's Password
New Password:
Retype New Password:
Miscellaneous
Remote Log Server:
Time Zone:
NTP Server:
pool.ntp.org
NTP Link
Apply

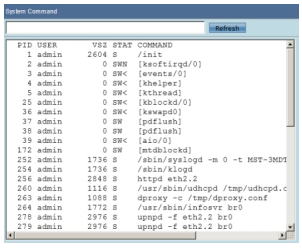

Operation Mode
System
Firmware Upgrade
Restore/Save/Upload Setting
Administration - Restore/Save/Upload Setting
Factory default
Restore
Save setting
Save
Upload setting
Upload
Browse...


General Log
DHCP leases
Wireless Log
Port Forwarding
Routing Table
System Log - General Log
System Time
Thu, Jan 01 00:51:45 1970 GMT+0300
Boot time
Clear
Save
Refresh

Now let's turn to the command line interface.

Command line interface

The command line interface is the same for both models. To access the System Command page, one has to add the following to the IP-address in the URL bar of the browser: Main_AdmStatus_Content.asp. This page allows running the commands of the built-in operating system. The account data for accessing System Command are the same as for the web-interface.


System Command
Refresh
PID USER VSZ STAT COMMAND
1 admin 2604 S /init
2 admin 0 SWN [ksoftirqd/0]
3 admin 0 SW< [events/0]
4 admin 0 SW< [khelper]
5 admin 0 SW< [kthread]
25 admin 0 SW< [kblockd/0]
36 admin 0 SW< [kswapd0]
37 admin 0 SW [pdflush]
38 admin 0 SW [pdflush]
39 admin 0 SW< [aio/0]
172 admin 0 SW [mtdblockd]
252 admin 1736 S /sbin/syslogd -m 0 -t MST-3MDT
254 admin 1736 S /sbin/klogd
256 admin 2848 S httpd eth2.2
260 admin 1116 S /usr/sbin/udhcpd /tmp/udhcpd.c
263 admin 1088 S dproxy -c /tmp/dproxy.conf
264 admin 1772 S /usr/sbin/infosvr br0
278 admin 2976 S upnpd -f eth2.2 br0
279 admin 2976 S upnpd -f eth2.2 br0

Besides this method, there's a traditional way to access the command line – with the help of Telnet. Unfortunately, it's impossible to disable this access.

There's a Busybox library version 1.12.1 installed on the router; to see the description and the list of supported commands, invoke *busybox*.

```
 #busybox
BusyBox v1.12.1 (2011-07-28 13:38:19 UTC) multi-call binary
Copyright (C) 1998-2008 Erik Andersen, Rob Landley, Denys Vlasenko
and others. Licensed under GPLv2.
See source distribution for full notice.
Usage: busybox [function] [arguments]...
or: function [arguments]...
BusyBox is a multi-call binary that combines many common Unix
```

utilities into a single executable. Most people will create a
link to busybox for each function they wish to use and BusyBox
will act like whatever it was invoked as!
Currently defined functions:
[, [[, ash, basename, brctl, cat, chmod, chpasswd, cp, date, echo,
expr, fdisk, free, ftpput, grep, hostname, ifconfig, insmod, kill,
killall, klogd, ln, logger, login, logread, ls, lsmod, mdev, mkdir,
mknod, mount, mv, ping, ps, pwd, rm, rmmod, route, sed, sh, sleep,
syslogd, telnetd, test, touch, traceroute, umount, vconfig, vi, wc

With the help of the *cat /proc/version* command we get information about the built-in operating system.

```
 #cat /proc/version
Linux version 2.6.21 (asus@localhost) (gcc version 3.4.2) #1016 Thu Sep 29 09:31:12 UTC 2011
```

The list of supported encryption types and file systems is in the */proc/crypto* and */proc/filesystems* files.

```
 #cat /proc/crypto
name         : ecb(arc4)
driver       : ecb(arc4-generic)
module       : kernel
priority     : 0
refcnt       : 1
type         : blkcipher
blocksize    : 1
min keysize  : 1
max keysize  : 256
ivsize       : 0
name         : arc4
driver       : arc4-generic
module       : kernel
priority     : 0
refcnt       : 1
type         : cipher
blocksize    : 1
min keysize  : 1
max keysize  : 256
name         : sha1
driver       : sha1-generic
module       : kernel
priority     : 0
```

```
refcnt          : 1
type            : digest
blocksize       : 64
digestsize      : 20
#cat /proc/filesystems
nodev    sysfs
nodev    rootfs
nodev    bdev
nodev    proc
nodev    sockfs
nodev    pipefs
nodev    futexfs
nodev    tmpfs
nodev    eventpollfs
nodev    devpts
 ext3
 ext2
 squashfs
nodev    ramfs
 vfat
nodev    fuse
 fuseblk
nodev    fusectl
```

Let’s obtain information about the device CPU and memory from the */proc/cpuinfo* and */proc/meminfo*
files.

```
  #cat /proc/cpuinfo
system type             : Ralink SoC
processor               : 0
cpu model               : MIPS 24K V4.12
BogoMIPS                : 212.99
wait instruction        : yes
microsecond timers      : yes
tlb_entries             : 32
extra interrupt vector  : yes
hardware watchpoint     : yes
ASEs implemented        : mips16 dsp
VCED exceptions         : not available
VCEI exceptions         : not available
#cat /proc/meminfo
MemTotal:        29072 kB
MemFree:         8320 kB
Buffers:         0 kB
```

```
Cached:         11980 kB
SwapCached:         0 kB
Active:          6644 kB
Inactive:        7360 kB
SwapTotal:          0 kB
SwapFree:           0 kB
Dirty:              0 kB
Writeback:          0 kB
AnonPages:       2060 kB
Mapped:          1520 kB
Slab:            4220 kB
SReclaimable:     864 kB
SUnreclaim:      3356 kB
PageTables:       360 kB
NFS_Unstable:       0 kB
Bounce:             0 kB
CommitLimit:     14536 kB
Committed_AS:     4768 kB
VmallocTotal:  1048404 kB
VmallocUsed:      1816 kB
VmallocChunk:  1045936 kB
```

Now, with the help of the *ps* command let's find out what processes are running on the router at the moment.

```
 #ps
PID USER       VSZ STAT COMMAND
1 admin     2596 S    /init
2 admin        0 SWN  [ksoftirqd/0]
3 admin        0 SW<  [events/0]
4 admin        0 SW<  [khelper]
5 admin        0 SW<  [kthread]
25 admin       0 SW<  [kblockd/0]
36 admin       0 SW<  [kswapd0]
37 admin       0 SW   [pdflush]
38 admin       0 SW   [pdflush]
39 admin       0 SW<  [aio/0]
172 admin      0 SW   [mtdblockd]
233 admin      0 SW   [RtmpWscTask]
252 admin   1732 S    /sbin/syslogd -m 0 -t GMT0 -O /tmp/syslog.log
254 admin   1732 S    /sbin/klogd
256 admin   2792 S    httpd eth2.2
260 admin   1116 S    /usr/sbin/udhcpd /tmp/udhcpd.conf
263 admin   1104 S    dproxy -c /tmp/dproxy.conf
264 admin   1772 S    /usr/sbin/infosvr br0
```

```
 282 admin     2592 S    usdsvr_broadcast
 283 admin     2592 S    usdsvr_unicast
 298 admin     1196 S    lld2d br0
 300 admin     1460 S    /usr/sbin/wanduck
 305 admin     2676 S    watchdog
 308 admin     2592 S    ntp
 311 admin     2592 S    ots
 328 admin     1732 S    telnetd
 330 admin     1440 S    detectWan_arp
 331 admin     1780 S    networkmap
 332 admin     1740 S    /bin/sh
 341 admin     1096 S    udhcpc -i eth2.2 -p /var/run/udhcpc0.pid -s /tmp/udhc
 592 admin     3024 S    upnpd -f eth2.2 br0
 594 admin     3024 S    upnpd -f eth2.2 br0
 595 admin     3024 S    upnpd -f eth2.2 br0
 598 admin     3024 S    upnpd -f eth2.2 br0
 599 admin     3024 S    upnpd -f eth2.2 br0
 600 admin     3024 S    upnpd -f eth2.2 br0
 602 admin     3024 S    upnpd -f eth2.2 br0
 603 admin     3024 S    upnpd -f eth2.2 br0
 605 admin     3024 S    upnpd -f eth2.2 br0
 606 admin     3024 S    upnpd -f eth2.2 br0
 638 admin     1732 S    sh -c ps > /tmp/syscmd.log 2>&1
 639 admin     1736 R    ps
```

With the help of the *ls* command let's see what files are located in the */bin* and */sbin*, */usr/bin* and
/usr/sbin
catalogues.

```
  # ls /bin
cp              hostname        ez-ipupdate     switch
date            grep            ntpclient       igmpproxy
chmod           iptables        rt2860apd       ls
reg             mtd_write       pwd             mv
flash           wscd            ln              mkdir
ping            touch           login           rm
echo            tc              iwconfig        mii_mgr
vi              iwpriv          ash             sh
sleep           umount          ps              upnp_xml.sh
busybox         sed             ated            iptables-restore
upnpd           kill            cat             mknod
mount           lld2d           igmpproxy.sh
# ls /sbin
udhcpc.sh                       gpio
```

tracktest radioctrl
ateshow usdsvr_broadcast
dhcpc_apply_delayed watchdog
getCurrentAddress lsmod
config.sh sta_wps_stop
config-l2tp.sh mdev
gen_ralink_config wan-down
getCountryCode gpio_rdint
restart_qos vconfig
gbe klogd
apcli_connect stopservice
rsrom syslogd
start_telnetd chpasswd.sh
FWRITE wps_oob
disktest getPIN
storage.sh wps_pbc
ejusb gpio_setbit
getIMG chkalltask
getSSID wps_start
config-igmpproxy.sh run_apps
config-udhcpd.sh halt
start_ddns rc
logread usdsvr_unicast
wan.sh ping_keep_alive
reboot nvram_restore
getApCliInfo gpio_wrint
config-dns.sh setDisassociate
ddns_updated atehelp
config-pptp.sh speedtest
route vpn-passthru.sh
getWPSAP ifconfig
restore start_mac_clone
global.sh stop_ftp
asuscfe write
ledon getStaConnectionSSID
ots start_ots
config-pppoe.sh gpio_setdir
getBootV fdisk
umount2 setBootV
startWan usbtpt
rmmod ip-up
wifi_unload.sh insmod
pspfix eject_usb1
get_sw convert_asus_values
greenap.sh dev_init.sh
restart_dns run_upnp

```
setMAC                          clearCountryCode
gbr                           ntp.sh
setCountryCode                  setPIN
getBSSID                      hotplug
apcli_monitor                 hotplug_usb_mass
ddns.sh                       wphy
wsrom                         ntp
test_of_var_files_in_mount_path  start_ntp
detectWan_arp                   sta_wps_pbc
getSiteSurvey                 getChannel
wan-up                        erase
run_ftp                       wmac
getTxPwrAll                     chkTxPwr
initial_var_file              ledoff
init                        wps_pin
automount.sh                    ip-down
wps_stop                      getMAC
nat.sh
# ls /usr/bin
logger      wc          traceroute  [          killall     test
basename    free        [[          ftpput      expr
# ls /usr/sbin
l2tp-control    wpa_cli         dproxy          wpa_supplicant
bpalogin        pptp            chpasswd        udpxy
tcpcheck        nvram           networkmap      l2tpd
infosvr         ntpclient       brctl           pptp.sh
wanduck         httpd           telnetd         pppd
udhcpd          udhcpc          pppoe-relay
```

Among the */usr/sbin* files there's the *nvram* utility. This command lets the user see and change the main parameters of the system operation.

```
  # nvram
usage: nvram [get name] [set name=value] [unset name] [show]
# nvram set http_passwd=1234
# nvram commit
```

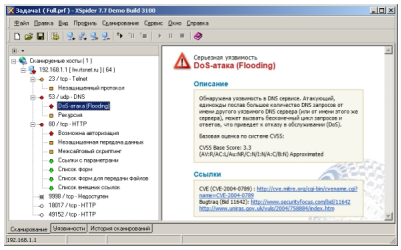
Now let's test the devices.

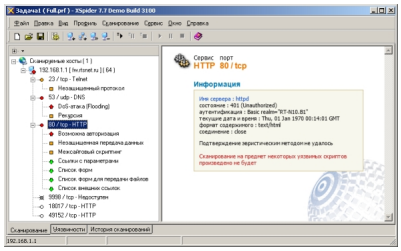
Testing

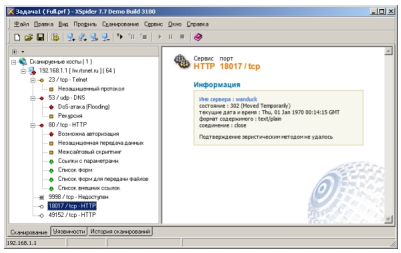
Traditionally, we start the testing section with determining the device booting time under which

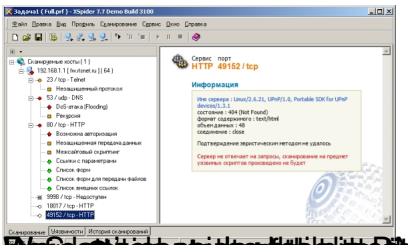
we mean the time interval between switching power on and receiving the first echo-reply via ICMP. ASUS RT-G32 rev.C1 and RT-N10 rev.B1 wireless routers boot in 35 seconds.

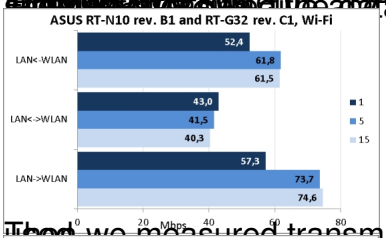
The next test is the device security against network attacks; for it we used a Positive Technologies XSpider 7.7 network security scanner (Demo build 3100). We scanned from the LAN-port. Altogether we discovered six open ports: TCP-23 (Telnet), UDP-53 (DNS), TCP-80 (HTTP), TCP-9998 (unavailable), TCP-18017 (HTTP) and TCP-49152 (HTTP). The most interesting information we discovered is presented below.

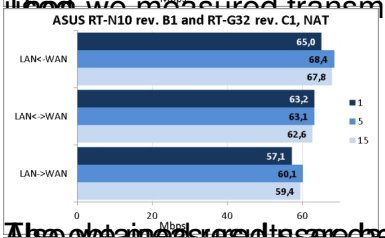


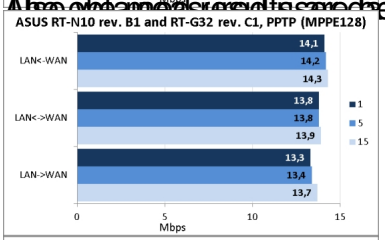


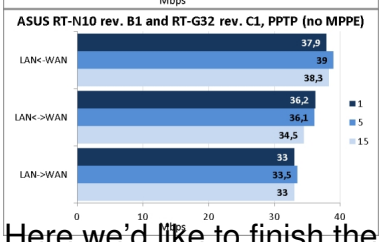












Here we'd like to finish the testing section and make conclusions.

Conclusion

So far in our testing lab we have only tested upmarket or middle-market models of ASUS wireless routers. The current material fills the gap and presents to our readers a review of low-cost wireless routaers with Fast Ethernet ports - ASUS RT-N10 rev. B1 and ASUS RT-G32 rev. C1. They are the cheapest devices of this vendor we've ever seen. Naturally, we didn't expect performance nywhere near that of upmarket products; however, the speeds we got were a nasty surprise. We think that ASUS RT-N10 rev. B1 and ASUS RT-G32 rev. C1 will suit only the most undemanding users or those whose budget is very limited. In all other cases we'd advise to turn to at least RT-N10U which we described in one of our reviews .

The advantages of the tested devices are listed below.

- Support of four wireless networks simultaneously
- Clear understandable interface
- Good transmission speeds in the wireless segment
- The possibility to manage bandwidth
- Support of authentication with the help of 802.1X MD5
- Affordable price

Unfortunately, we can’t but point out the disadvantages of the models at hand.

- Low transmission speeds if NAT/PAT is used
- Incorrect time zones for Moscow and some other Russian cities
- Impossibility to set Cyrillic names for NTP and VPN servers
- Impossibility to disable telnet-access to the device
- Lack of utilities for RT-G32 rev. C1 on the vendor’s site

When the article was being written the average price for ASUS RT-G32 rev.C1 and RT-N10 rev.B1 in Moscow online shops was 1250 RUB.